IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	David J. Allard	Confirmation No.:	9891
Application No.	10/780,098	Examiner:	Rangrej, Sheetal
Date filed:	February 17, 2004	Group:	3686
For:	Method, system, and apparatus for patient controlled access of medical records		

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

Sir:

This Appeal Brief is being filed concurrently with a Notice of Appeal on February 25, 2010. The Patent Office is expressly authorized to charge any fees under 37 C.F.R. § 41.20(b) to Deposit Account No. 14-1437.

37 C.F.R. § 41.37(c)(1)(i) *Real Party in Interest*

The real party in interest is International Business Machines Corporation (IBM), the assignee of record. The assignment has been recorded by the USPTO on March 15, 2004, at Reel No. 014426, Frame No. 0552.

37 C.F.R. § 41.37(c)(1)(ii) *Related Appeals and Interferences*

No related appeals or interference proceedings are currently pending which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

37 C.F.R. § 41.37(c)(1)(iii) *Status of Claims*

Claims 1, 3-4, 16-18, 20, 22-24, and 26-27 are rejected and are being appealed. Claims 2, 5-15, 19, 21, and 25 have been cancelled.

37 C.F.R. § 41.37(c)(1)(iv) *Status of Amendments*

No claims were amended after the final Office action.

37 C.F.R. § 41.37(c)(1)(v) *Summary of Claimed Subject Matter*

Independent claim 1 of the instant application recites a computer-implemented method of permitting controlled access to medical information of a patient (see, for example, paragraph [0014], lines 1-2 of the specification), the method comprising:

supplying medical information of the patient to a central repository by the patient and any medical providers who have treated the patient (see, for example, paragraph [0017], lines 2-3);

storing and maintaining the medical information of the patient in the central repository (see, for example, paragraph [0016], lines 2-4);

accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN (see, for example, paragraph [0017],line 4, and paragraph [0018], lines 1-2);

controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed (see, for example, paragraph [0023]);

assigning each authorized user with a unique authorized user ID and an authorized user PIN (see, for example, paragraph [0024], lines 1-3); and

tracking and notifying the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information (see, for example, paragraph [0035]).

Independent claim 20 of the instant application recites a machine-readable storage having stored thereon, a computer program having a plurality of code sections, said code sections executable by a machine for causing the machine to perform the steps of (see, for example, paragraph [0010], lines 1-4 of the specification):

supplying medical information of the patient to a central repository by the patient and any medical providers who have treated the patient (see, for example, paragraph [0017], lines 2-3);

storing and maintaining the medical information of the patient in the central repository (see, for example, paragraph [0016], lines 2-4);

accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN (see, for example, paragraph [0017], line 4, and paragraph [0018], lines 1-2);

controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed (see, for example, paragraph [0023]);

assigning each authorized user with a unique authorized user ID and an authorized user PIN (see, for example, paragraph [0024], lines 1-3); and

tracking and notifying the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information (see, for example, paragraph [0035]).

Independent claim 24 of the instant application recites a computer-implemented system for permitting controlled access to medical information of a patient (see, for example, paragraph [0014], lines 1-2 of the specification), the system comprising:

a central repository for storing and maintaining medical information of the patient, the medical information of the patient being supplied to the central repository by the patient and any medical providers who have treated the patient (see, for example, paragraph [0017], lines 1-3);

an access device for accessing the medical information by the patient or any other authorized user, the patient accessing the medical information from the access device using a unique patient identifier and a patient PIN, each authorized user accessing the medical information from the access device using a unique authorized user ID and an authorized user PIN (see, for example, paragraph [0017], line 4, and paragraph [0018], lines 1-2); and

at least a processor configured to

control by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed (see, for example, paragraph [0023]);

assign each authorized user with a unique authorized user ID and an authorized user PIN (see, for example, paragraph [0024], lines 1-3); and

track and notify the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information (see, for example, paragraph [0035]).

37 C.F.R. § 41.37(c)(1)(vi) *Grounds of Rejection to be Reviewed on Appeal*

1. Whether claims 1, 3-4, 20, 22-24, and 26-27 are patentable under 35 U.S.C. § 103(a) over U.S. Patent 6,988,075 to Hacker, *et al.* (hereinafter Hacker) in view of non-patent literature, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, Feb. 2001; 322, pages 283-287 to Mandl, *et al.* (hereinafter Mandl).
2. Whether claims 16-18 are patentable under 35 U.S.C. § 103(a) over Hacker in view of Mandl, and further in view of U.S. Published Patent Application 2002/0010679 to Felsher (hereinafter Felsher).

37 C.F.R. § 41.37(c)(1)(vii) *Argument*

Claims 1, 3-4, 20, 22-24, and 26-27 are patentable over Hacker in view of Mandl under 35 U.S.C. § 103(a)

Claims 1, 20, and 24

It was asserted in the final Office Action that Hacker discloses a system having a unique access identification means (i.e. unique ID) and also giving a pass phrase to access the system (i.e. pin). Hacker teaches providing the provider with appropriate means for input of the unique access identification for patient identification and access along with unique passphrases (i.e. pin) to access the patient information (Hacker: col. 7, 60-66).

Col. 7, lines 60-66 of Hacker reads:

> *Appropriate means for input of the unique access identification means, such as bar code readers (BCRs) 160 for bar coded cards and bracelets, can be used for patient identification and access. Particularly sensitive patient information can be passphrase protected so that the medical provider must get permission from the patient to gain access to it.*

In Hacker the unique access identification means is used for patient identification and is thus unique to the patient. The passphrase is used to get permission from the patient to gain access to sensitive patient information. Therefore, in Hacker both the access identification means and the passphrase are unique to the patient whose information is being accessed. In contrast, in the present invention, aside from the unique patient identifier and the patient PIN provided to the patient, an authorized user, such as a medical provider, is provided with a unique authorized user ID and an authorized user PIN to access the patient information when the patient is not around (see, e.g., paragraph [0024] of the specification of the instant application).

It was asserted in the final Office Action that Mandl discloses the patient having preferences about different parts of his/her medical history by providing authorization independently; furthermore teachings that patients grant different access rights to different providers based on their role and on the particular individual (Mandl: p. 284; section Confidentiality).

Although Mandl mentions that the patient can limit the information to specific providers and provides an override mechanism that is controlled by the patient, Mandl does not suggest using an access control list as the mechanism for controlling access. It is noted that granting different access rights to different providers based on their role is not the same as using an access control list as the mechanism for controlling access. The former is the result and the latter is the tool to achieve the result. More specifically, Mandl does not disclose controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, and wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed, as recited in Claims 1, 20, and 24 of the instant application.

In addition, since Hacker does not provide an authorized user, such as a medical provider, with a unique authorized user ID and an authorized user PIN to access the patient information when the patient is not around, Hacker cannot track and notify the

patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information. It is described in col. 7, line 66 to col. 8, line 3 of Hacker that the patient can also specify an emergency override of passphrase protection, and notification to the patient can be provided as to what information was released to emergency medical personnel, including time, location, pages accessed, etc. However, it is noted that the system of Hacker cannot track the identity of the user who accessed the medical information because the emergency medical personnel does not have an authorized user ID.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claims 1, 20, and 24. Applicants therefore respectfully submit that Claims 1, 20, and 24 define over the prior art. Furthermore, as each of the remaining claims depends from Claims 1, 20, or 24 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Claims 3-4, 22-23, and 26-27

Regarding claims 3, 22, and 26, Hacker suggests the use of a bar code or patient ID card, but does not teach a universally unique identifier. Rather, Hacker teaches an identifier that could be specific only to a particular record system, such as in current hospital systems; the same patient wrist codes (MRN, or Account) may refer to different patients at different hospitals.

Regarding claim 4, 23, and 27, Hacker proposes an override for emergency situations but does not teach the mechanism of registration of emergency providers that would prevent the access to information by those searching for private information and posing to be an emergency provider.

Claims 3-4, 22-23, and 26-27 are also believed to be patentable because of their dependency on patentable independent claims 1, 20, and 24, respectively.

Claims 16-18 are patentable over Hacker in view of Mandl and further in view of Felsher under 35 U.S.C. § 103(a)

Claims 16-18

Regarding claim 17, Felsher describes in paragraph [0354] that once a password is verified, the user is authenticated for the duration of the session, or possibly with a maximum timeout limit, such as 15 minutes, whichever is shorter. However, Felsher does not disclose that during a doctor visit the patient provides access to the medical information for a time period long enough to support the visit at which point the access times out. It is noted that in Felsher the system determines the length of the session whereas in the present invention the patient controls the length of the session.

Regarding claims 18, this claim describes a key feature in a typical doctor's office visit, where computers are provided in each of the patient examining rooms for the direct access and recording of patient private information. When the doctor moves to another room the access to patient information needs to be protected from other patients who might seize the opportunity to browse another's private information. The mechanism of

logging into another examining room should immediately prevent access from a prior terminal.

Felsher describes in paragraph [0359] that in the CareWeb system, in addition to storing encrypted username and password information, the security cookie contains the job role of the user; this may pose security threats, for example if the security cookie is borrowed from the client machine, and employed in a second communication session within the time limit parameters. It is not clear how this has anything to do with the limitation of claim 18, namely that access to the patient's medical information expires when a physician logs into another room/appointment

Claims 16-18 are also believed to be patentable because of their dependency on patentable independent claim 1.

In view of the forgoing, the honorable Board is therefore respectfully urged to reverse the final rejection of the Primary Examiner.

Respectfully submitted,

NOVAK DRUCE + QUIGG LLP

Date: February 25, 2010

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
525 Okeechobee Blvd., 15th Floor
West Palm Beach, FL 33401
Telephone: (561) 847-7800

37 C.F.R. § 41.37(c)(1)(viii) *Claims Appendix*

1. A computer-implemented method of permitting controlled access to medical information of a patient, the method comprising:

supplying medical information of the patient to a central repository by the patient and any medical providers who have treated the patient;

storing and maintaining the medical information of the patient in the central repository;

accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN;

controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed;

assigning each authorized user with a unique authorized user ID and an authorized user PIN; and

tracking and notifying the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information.

3. The method of claim 1, wherein the access device is controlled using a universally unique identifier.

4. The method of claim 1, wherein said controlling step is overridden by a registered emergency provider.

16. The method of claim 1, wherein the patient is compensated for permitting some of the medical information to be available and used by a research institution.

17. The method of claim 1, wherein during a doctor visit the patient provides access to the medical information for a time period long enough to support the visit at which point the access times out.

18. The method of claim 1, wherein access to the patient's medical information expires when a physician logs into another room/appointment.

20. A machine-readable storage having stored thereon, a computer program having a plurality of code sections, said code sections executable by a machine for causing the machine to perform the steps of:

supplying medical information of the patient to a central repository by the patient and any medical providers who have treated the patient;

storing and maintaining the medical information of the patient in the central repository;

accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN;

controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed;

assigning each authorized user with a unique authorized user ID and an authorized user PIN; and

tracking and notifying the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information.

22. The machine-readable storage of claim 20, wherein the access device is controlled using a universally unique identifier.

23. The machine-readable storage of claim 20, wherein said controlling step is overridden by a registered emergency provider.

24. A computer-implemented system for permitting controlled access to medical information of a patient, the system comprising:

a central repository for storing and maintaining medical information of the patient, the medical information of the patient being supplied to the central repository by the patient and any medical providers who have treated the patient;

an access device for accessing the medical information by the patient or any other authorized user, the patient accessing the medical information from the access device using a unique patient identifier and a patient PIN, each authorized user accessing the medical information from the access device using a unique authorized user ID and an authorized user PIN; and

at least a processor configured to

control by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed;

assign each authorized user with a unique authorized user ID and an authorized user PIN, and

track and notify the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information.

26. The system of claim 24, wherein the access device is controlled using a universally unique identifier.

27. The system of claim 24, wherein the access control is overridden by registered emergency providers.

37 C.F.R. § 41.37(c)(1)(ix) ***Evidence Appendix***

None.

37 C.F.R. § 41.37(c)(1)(x) *Related proceedings Appendix*

None.